The SETHEO System

Ortrun Ibens

Institut für Informatik, Technische Universität München
ibens@informatik.tu-muenchen.de

1 Overview

SETHEO [LSBB92, GLMS94, MIL+97] is a theorem prover for first-order predicate logic. The SETHEO system includes an efficient inference machine with a preprocessing module for a specialized equality handling and a graphical proof display. Furthermore, Prolog-style built-ins are provided for logic-programming. The system is being continuously extended and enhanced with additional inference mechanisms and reduction techniques. The current version of SETHEO is V4.0.

2 The Inference Machine

SETHEO is a top-down prover based on the calculus of so-called *connection tableaux* [LMG94] which generalizes *weak model elimination* [Lov78]. Proofs are found by a consecutively bounded depth-first iterative deepening search with backtracking [Sti88]. The search procedure is implemented as an abstract machine which extends the Warren Abstract Machine.

A connection tableau for a set of clauses is generated by first applying the *start rule* and then repeatedly applying either the *reduction* or the *extension rule*. Employment of the start rule means the selection of a clause from a set of possible start clauses and attaching its literals to the root node. The extension rule requires the performance of a unification step which entails attaching the (instantiated) literals of a *connected clause* to the current subgoal K, i.e., a clause that contains a literal which can be unified with the complement of K. The reduction rule permits the closing of a branch by unifying a subgoal with the complement of a literal on the branch.

As an additional inference rule, the *folding up* operation [LMG94], which corresponds to Shostak's *c-reduction* [Sho76], is integrated. This rule provides a restricted but highly efficient kind of lemma generation. To prevent redundancies, regularity and tautology-freeness are enforced and clause- and tableau-subsumption are avoided [LSBB92, LMG94]. Furthermore, elaborate techniques for clause and subgoal selection are applied [IL97].

3 Equality Handling

A traditional weakness of calculi of the model elimination type is the handling of equality. Since the most successful paradigms for treating equality in saturation-based theorem proving, i.e., *paramodulation* [RW69] and its refined versions [BGLS95], are not complete in a goal-directed setting, SETHEO's equality handling is based on *lazy basic paramodulation* [GS89], a variant of paramodulation which is compatible with model elimination. This method is implemented by means of a transformation from input formulae with equality axioms into formulae without equality [MS97], which are then processed by the standard inference machine. Interestingly, this transformation is a variant of the STE-modification developed by Brand [Bra75].

4 Applications and User Support

SETHEO has been successfully used for case studies, e.g., protocol verifications [Sch95]. Furthermore, SETHEO has been integrated into the ILF system for interactive proof generation and editing [DGH+94], and into the tool NORA/HAMMR for software reuse [FKS95]. SETHEO was the winner of the ATP system competition held at CADE-13 [SS97].

Since SETHEO is based on Prolog abstract machine technology, it can also be applied for logic-programming. A set of Prolog-style built-ins and additional features (like backtrackable global variables) are provided and can be combined with the basic theorem proving techniques of SETHEO (e.g., sound unification, access of the current path in the tableau, iterative deepening).

The SETHEO system includes an X-based graphical user interface which can be used to display the proof tree (a tableau with applied substitutions). Features for scrolling and hiding parts of the tableau allow the representation of even extremely large tableaux in a readable manner. The system is implemented in C rsp. in Eclipse-Prolog as a set of independent programs. Binaries for different platforms can be obtained from `ftp.informatik.tu-muenchen.de` in directory `/local/lehrstuhl/jessen/Automated_Reasoning/SETHEO`. A draft version of the reference manual [SI97] is available on request.

References

[BGLS95] L. Bachmair, H. Ganzinger, C. Lynch, W. Snyder. Basic Paramodulation. *Information and Computation*, 121(2):172–192, 1995.

[Bra75] D. Brand. Proving theorems with the modification method. *SIAM J. Comp.*, 4(4):412–430, 1975.

[DGH+94] B. I. Dahn, J. Gehne, T. Honigmann, L. Walther, A. Wolf. Integration of Automated and Interactive Theorem Proving in ILF. In *Proceedings of CADE-14*, LNAI. Springer, to appear 1997.

[FKS95] B. Fischer, M. Kievernagel, G. Snelting. Deduction-Based Software Component Retrieval. In *IJCAI-95 Workshop on Formal Approaches to the Reuse of Plans, Proofs, and Programs*, Montreal, Canada, 1995.

[GLMS94] C. Goller, R. Letz, K. Mayr, J. Schumann. SETHEO V3.2: Recent Developments – System Abstract –. In *Proceedings of CADE-12*, LNAI 814, p. 778–782. Springer, 1994.

[GS89] J. Gallier, W. Snyder. Complete Sets of Transformations for General e-Unification. *Theoretical Computer Science*, 67:203–260, 1989.

[IL97] O. Ibens, R. Letz. Subgoal Alternation in Model Elimination. In *TABLEAUX'97*, LNAI 1227, p. 201–215. Springer, 1997.

[LMG94] R. Letz, K. Mayr, C. Goller. Controlled Integration of the Cut Rule into Connection Tableau Calculi. *JAR*, 13:297–337, 1994.

[Lov78] D. W. Loveland. *Automated theorem proving: A logical basis.* North Holland, New York, 1978.

[LSBB92] R. Letz, J. Schumann, S. Bayerl, W. Bibel. SETHEO: A High-Performance Theorem Prover. *JAR*, 8:183–212, 1992.

[MIL+97] M. Moser, O. Ibens, R. Letz, J. Steinbach, C. Goller, J. Schumann, K. Mayr. SETHEO and E-SETHEO – The CADE-13 Systems. JAR, 18:237–246, 1997.

[MS97] M. Moser, J. Steinbach. Compiling basic paramodulation to logic. Technical report, Institut für Informatik, TU München, to appear 1997.

[RW69] G. A. Robinson and L. Wos. Paramodulation and theorem proving in first-order theories with equality. *Machine Intelligence*, 4:135–150, 1969.

[Sch95] J. Schumann. Using the Theorem Prover SETHEO for Verifying the Development of a Communication Protocol in FOCUS: A Case Study. *TABLEAUX'95*, LNAI 918, 338–352. Springer, 1995.

[Sho76] R. E. Shostak. Refutation graphs. *Artificial Intelligence*, 7:51–64, 1976.

[Sti88] M. E. Stickel. A Prolog technology theorem prover: Implementation by an extended Prolog compiler. *JAR*, 4:353–380, 1988.

[SI97] J. Schumann, O. Ibens. *SETHEO V3.3 Reference Manual.* Institut für Informatik, TU München, to appear 1997.

[SS97] G. Sutcliffe, C. B. Suttner. The Results of the CADE-13 ATP System Competition. *JAR*, 18:271–286, 1997.